VSB – Technical University of Ostrava
Faculty of Electrical Engineering and Computer Science
Department of Computer Science

Diploma Thesis Assignment

Student: **Maksim Kirei**

Study Programme: N0612A140005 Information and Communication Security

Title: Malware Analysis from the Behavioral Point of View
Analýza malware z pohledu behaviorálních charakteristik

The thesis language: English

Description:

The aim of the work is to collect a representative set of malware descriptions according to families determined by the supervisor in the widest possible range. Furthermore, on this data to perform analysis, visualization of statistical surveys and possible identification of typical features of behaviour according to the assignment of the DP supervisor. Part of the solution is the search for atypical traits of behaviour and their classification. It is assumed for student to use both classical methods and selected methods in the field of soft computing. The expected structure of the work is therefore as follows:

1. Current state in the field of data processing and analysis.
2. Defining suitable data sources and selecting samples whose behaviour is to be analyzed.
3. Data collection.
4. Preliminary analysis and data visualization.
5. Selection of suitable methods for analysis and identification of viral sequences and their families.
6. Execution of the experiment.
7. Evaluation of results.
8. Conclusion.

References:

[1] Rieck, K., Trinius, P., Willems, C. and Holz, T., 2011. Automatic analysis of malware behavior using machine learning. Journal of Computer Security, 19(4), pp.639-668.
[2] Firdausi, I., Erwin, A. and Nugroho, A.S., 2010, December. Analysis of machine learning techniques used in behavior-based malware detection. In 2010 Second international conference on advances in computing, control, and telecommunication technologies (pp. 201-203). IEEE.
[3] Gavriluţ, D., Cimpoeşu, M., Anton, D. and Ciortuz, L., 2009, October. Malware detection using machine learning. In 2009 International Multiconference on Computer Science and Information Technology (pp. 735-741). IEEE.
[4] Makandar, A. and Patrot, A., 2015, December. Malware analysis and classification using artificial neural network. In 2015 International conference on trends in automation, communications and computing technology (I-TACT-15) (pp. 1-6). IEEE.
[5] Bezobrazov, S. and Golovko, V., 2014. Artificial immune systems approach for malware detection: neural networks applying for immune detectors construction. International Journal of Computing, 7(2), pp. 44-50.

Extent and terms of a thesis are specified in directions for its elaboration that are opened to the public on the web sites of the faculty.

Supervisor: **prof. Ing. Ivan Zelinka, Ph.D.**

Date of issue: 01.09.2020

Date of submission: 30.04.2021

prof. Ing. Jan Platoš, Ph.D.
Head of Department

prof. Ing. Pavel Brandštetter, CSc.
Dean